MATH 240: Discrete Structures - Assignment 3

Liam Scalzulli
liam.scalzulli@mail.mcgill.ca

November 7, 2022

Problem 1

Proof. Assume $2^n - 1$ is prime.

Let $\sigma(n)$ be a function that computes the sum of all divisors of a given number n.

Then $\sigma(2^n - 1) = 2^n$ since the only divisors of $2^n - 1$ are 1 and $2^n - 1$ as a result of $2^n - 1$ being prime:

$$1 + 2^n - 1 = 2^n$$

Moreover, we have $\sigma(2^{n-1}) = 2^n - 1$ as the divisors of 2^{n-1} are all powers of 2 up to and including 2^{n-1}:

$$\begin{aligned} &1 + 2 + 4 + 8 + ... + 2^{n-1} \\ &= 2^0 + 2^1 + 2^2 + 2^3 + ... + 2^{n-1} \end{aligned}$$

The above is just a geometric series, whose sum can be computed using the formula $S_n = \frac{1-r^{n+1}}{1-r}$ (source: https://mathworld.wolfram.com/GeometricSeries.html) where r is the common ratio, and n is the number of terms.

In this case, $r = 2$ and $n = n - 1$. This gives us enough information to compute the sum:

$$\begin{aligned} S_n &= \frac{1 - 2^{(n-1)+1}}{1 - 2} \\ &= \frac{1 - 2^n}{-1} \\ &= 2^n - 1 \end{aligned}$$

Lastly, we must notice that our function $\sigma(n)$ is multiplicative, that is $\sigma(ab) = \sigma(a) \cdot \sigma(b)$, if a and b are relatively prime. I won't prove this here, but link to a wikipedia article that explains more about the function and its properties: https://en.wikipedia.org/wiki/Divisor_function.

For the purposes of this proof, we know that $2^n - 1$ and 2^{n-1} are relatively prime, so our function $\sigma(n)$ is multiplicative for the numbers $2^n - 1$ and 2^{n-1}.

Putting it all together:

$$\begin{aligned} \sigma(2^{n-1}(2^n - 1)) &= \sigma(2^{n-1})\sigma(2^n - 1) && \text{[Multiplicative property]} \\ &= (2^n - 1)(2^n) && \text{[Replace with sums]} \\ &= 2(2^{n-1})(2^n - 1) && \text{[Factor out a 2]} \end{aligned}$$

Therefore $2^n - 1(2^n - 1)$ is a perfect number as $\frac{\sigma(2^{n-1}(2^n-1))}{2} = 2^{n-1}(2^n - 1)$. $\square$

Problem 2

Step 1: Find $148^{-1} \pmod{421}$

Compute the steps of the Euclidean GCD algorithm:

$$\begin{aligned}
421 &= 2 \times 148 + 125 \\
148 &= 1 \times 125 + 23 \\
125 &= 5 \times 23 + 10 \\
23 &= 2 \times 10 + 3 \\
10 &= 3 \times 3 + 1
\end{aligned}$$

Roll back the steps to find $s, t \in \mathbb{Z}$ such that $1 = 421s + 148t$

$$\begin{aligned}
1 &= 1(10) - 3(3) \\
&= 1(10) - 3(23 - 2(10)) \\
&= 7(10) - 3(23) \\
&= 7(125 - 5(23)) - 3(23) \\
&= 7(125) - 38(23) \\
&= 7(125) - 38(148 - 1(125)) \\
&= 45(125) - 38(148) \\
&= 45(421 - 2(148)) - 38(148) \\
&= 45(421) - 128(148)
\end{aligned}$$

So $1 = 45(421) - 128(148)$, we then get $1 = -128(148)$, hence $148^{-1} \pmod{421} \equiv -128 \equiv 293 \pmod{421}$.

Step 2: Solve $148x \equiv 12 \pmod{421}$

$$\begin{aligned}
148x &\equiv 12 \pmod{421} \\
x &\equiv 12 \times 293 \pmod{421} \\
&\equiv 3516 \pmod{421} \\
&\equiv 148 \pmod{421}
\end{aligned}$$

Problem 3

Recall: $a^{p-1} \equiv 1$ (mod p)

(a)

First we try to decompose 1335 into $(18 \cdot n) + r$.

$$\begin{array}{r}
74 \\
18\,\overline{)1335} \\
\underline{126} \\
75 \\
\underline{72} \\
3
\end{array}$$

Therefore $n = 74$ and $r = 3$

$$\begin{aligned}
2409^{1335} \pmod{19} &= 2409^{(18\cdot 74)+3} \pmod{19} \\
&= 2409^{3} \pmod{19} && [2409 \equiv 15 \pmod{19} \text{ by LD}] \\
&= 15^{3} \pmod{19} \\
&= 3375 \pmod{19} && [\text{Perform LD on } (3375,\ 19)] \\
&= 12 \pmod{19}
\end{aligned}$$

(b)

First we try to decompose 42806 into $(348 \cdot n) + r$.

$$\begin{array}{r}
123 \\
348\,\overline{)42806} \\
\underline{348} \\
800 \\
\underline{696} \\
1046 \\
\underline{1044} \\
2
\end{array}$$

Therefore $n = 123$ and $r = 2$.

$$\begin{aligned}
7^{42806} \pmod{349} &= 7^{(123\cdot 348)+2} \pmod{349} \\
&= 7^{2} \pmod{349} \\
&= 49 \pmod{349}
\end{aligned}$$

Problem 4

(a)

$$\begin{aligned}\hat{M} &= M^p \text{ mod n} \\ &= 4^5 \text{ mod } 91 \\ &= 1024 \text{ mod } 91 \\ &= 23\end{aligned}$$

(b)

$$\begin{aligned}x &= p^{-1} \text{ mod } (q_1 - 1)(q_2 - 1) \\ &= 5^{-1} \text{ mod } 72\end{aligned}$$

Compute the steps of the Euclidean GCD algorithm:

$$\begin{aligned}72 &= 14 \times 5 + 2 \\ 5 &= 2 \times 2 + 1\end{aligned}$$

Roll back the steps to find $s, t \in \mathbb{Z}$ such that $1 = 5s + 72t$

$$\begin{aligned}1 &= 5 - 2(2) \\ &= 5 - 2(72 - 14(5)) \\ &= 29(5) - 2(72)\end{aligned}$$

So we see that $x = 29$, since $p \cdot 29 \equiv 1 \text{ mod } 72$.

(c)

$$\begin{aligned}M &= \hat{M}^x \text{ mod n} \\ &= 23^{29} \text{ mod } 91\end{aligned}$$

We know that $91 = 7 \cdot 13$, therefore by the Chinese Remainder Theorem a solution to 23^{29} mod 7 is also a solution to our original equation:

$$\begin{aligned}M &= \hat{M}^x \text{ mod n} \\ &= 23^{29} \text{ mod } 91 \\ &= 23^{29} \text{ mod } 7 \\ &= 23^{(7 \cdot 3)+2} \text{ mod } 7 \\ &= 23^2 \text{ mod } 7 \\ &= 529 \text{ mod } 7\end{aligned}$$

Perform long division on the integers 529 and 7:

$$
\begin{array}{r}
75 \\
7\,\overline{)\,529} \\
\underline{49} \\
39 \\
\underline{35} \\
4
\end{array}
$$

Therefore our answer is 4.